TNI Module Four

Other Network Security Services

This module is the fourth of four modules that describe the use of the Trusted Network Interpretation (TNI) of the Trusted Computer System Evaluation Criteria (TCSEC) for network product evaluation and certification. The basic terms and concepts presented in the TNI are summarized in TNI Module One. TNI Module Two presents Part I of the TNI, which provides TCSEC interpretations for complete network systems. TNI Module Three describes the rationale for NTCB partitions and interpretations of the TCSEC for network component evaluations presented in Appendices A and B of the TNI. A network system or component may also offer other security services (e.g., non-repudiation, denial of service). These security services and guidelines for their ratings are presented here, in TNI Module Four.

Module Learning Objectives

This module describes the additional network security features discussed in the TNI Part II. Communications Integrity, Denial of Service, and Compromise protection services are introduced and the special treatment required for their evaluation, as opposed to a TCSEC evaluation, is explained. Finally, working examples are described.

This module assumes an understanding of basic networking and the ISO OSI model. Upon completion of this module, the student should understand:

1) why the other services are rated, who uses them, and why they are useful.

2) the types of other security services applicable to a networking environment and the threats they address.

3) why these services cannot be evaluated via a TCSEC interpretation

4) the basis and methods for NCSC service assessment and the features examined.

Overview

Part I of the TNI concentrates on control of access to information on a standalone basis in the context of TCSEC requirements. A network environment, however, introduces additional concerns beyond those of standalone systems. Information is made more available to the outside world. The information is, at times, traveling across media that is shared by many known and unknown users, and may be susceptible to unreliable transmission. As a result, additional threats are introduced. It is the evaluation of a systems protection against these threats that is described by TNI Part II.

In this module, examples using existing products will be given when applicable. There are several secure LAN products in the market. The Verdix Secure LAN (VSLAN) is a NCSC evaluated, B2 MDIA secure LAN component.

It also provides some of the other security services to be discussed in this module. The VSLAN is implemented by the installation of Network Security Devices in each host and the inclusion of a PC-based Verdix Network Security Center (NSC). It provides security at the data link layer and below. The NSDs enforce access control at each host as well as provide audit data to the NSC. The NSC provides the network management functions. The Boeing MLS LAN SNS is a NCSC evaluated A1 MI secure LAN component which also includes some other security services. The MLS LAN is implemented through the connection of hosts to a Secure Network Server (SNS). Access control is enforced between hosts via controls in each host's connected SNS. The Boeing MLS LAN, which includes a Network Management Node, is currently being evaluated at the A-level. The Blacker Front End (BFE), the Motorola Network Encryption System (NES), the Xerox Encryption Unit (XEU), and the Wang Trusted Interface Unit (TIU) provide level 1 end-to-end encryption. The KG-84 is used for link encryption and is distributed by NSA. The Harris CS/SX is currently under B-level evaluation and has included its secure networking functions in the evaluation. The GOSIP compliant Secure Data Network System (SDNS) was developed by NSA. SDNS is a protocol that specifies security services at many OSI layers.

The threats can be characterized by three major categories:

- Communications integrity,
- Denial of Service, and
- Data compromise.

Communications integrity concerns the accuracy and believability of both the data and the source of the data. Communications integrity may be compromised via both malicious attack (active wiretapping) and unreliable communications.

Denial of Service, as the name implies, is the disruption of the network so that throughput falls below an acceptable level, the extreme case being the total loss of access to one or all of the remote entities. Denial of Service may be effected by unreliable transmission media, jamming, overloading, or physical disconnection of cables.

Data compromise involves the direct disclosure of information as well as the disclosure of information through analysis of network activity. Data may be compromised by observation of the data via passive wiretapping or by traffic flow analysis.

Systems counter some or all of these threats in a variety of ways. Most threats can be eliminated by physical protection of the transmission media and many secure network components have made this basic assumption. In some cases this may be an acceptable solution where either the media is easily protected or it is not necessary, such as aboard an airplane. However, where the transmission media passes through an unprotected environment, additional services may be deemed necessary.

The Other Security Services are grouped in the TNI as Communications Integrity Services, Denial of Service Protection, and Compromise Protection. These services cannot be evaluated as a TCSEC interpretation and the nature of these services prevents the assignment of a quantitative rating scale similar to that used in Part I. This is for several reasons. In many cases, the threats addressed by these services are out of scope of Part I. Also, some threats lack the measure of theoretical basis and formal analysis that drove the Part I requirements and rating scale. Further, some services may be provided by mechanisms outside of the TCB. As a result, a qualitative assessment of the services is performed, as opposed to the quantitative, hierarchical ratings that result from Part I. A rating of "none", "minimum", "fair" and "good" will be assigned in the evaluation. When appropriate, the service may be described as simply "not offered" or "present".

The evaluation criteria are grouped under three categories:

- Functionality,
- Strength of Mechanism, and
- Assurance.

Functionality concerns the service's objectives and the approach to satisfy those objectives. The features, mechanisms, and performance necessary to provide the service are delineated in Part II. This rating is based mostly on the presence of required mechanisms.

Strength of mechanism rates how well the approach achieves its objectives. As an example, there are different forms of encryption that provide data confidentiality, but some are more "robust" than others. The same mechanism is used, but some implementations are stronger than others. This rating is based on the type of mechanisms used as well as the correctness of the protocol logic.

The assurance rating provides a basis for believing that the functionality has been implemented correctly and that the objectives of the service have been achieved. This rating is closely tied to the rating achieved in Part I and includes meeting reference monitor requirements. The rating is derived from analysis and testing.

The possible ratings for each service, based on these criteria, are shown in Table 4-1.

Network Security Service		Criterion	Evaluation
Section	Title		Range
9.1	Communications Integrity		
9.1.1	Authentication	Functionality	None, present
		Strength	None to good
		Assurance	None to good
9.1.2	Communications Field Integrity	Functionality	None to good
		Strength	None to good
		Assurance	None to good
9.1.3	Non-repudiation	Functionality	None, present
		Strength	None to good
		Assurance	None to good
9.2	Denial of Service		
9.2.1	Continuity of Operations	Functionality	None to good
		Strength	None to good
		Assurance	None to good
9.2.2	Protocol Based Protection	Functionality	None to good
		Strength	None to good
		Assurance	None to good
9.2.3	Network Management	Functionality	None to good
		Strength	None to good
		Assurance	None to good
9.3	Compromise Protection		
9.3.1	Data Confidentiality	Functionality	None, present
		Strength	Max Sensitivity level
		Assurance	None to good
9.3.2	Traffic Confidentiality	Functionality	None, present
		Strength	Max Sensitivity level
		Assurance	None to good
9.3.4	Selective Routing	Functionality	None, present
		Strength	None to good
		Assurance	None to good

Table 4-1: TNI Evaluation Structure for the Network Security Services

These ratings supply information to the system accreditor as to the suitability of the evaluated system to their specific environment. Each environment will involve a unique set of threats. As an example, a system integrator may feel that data could not be compromised by the analysis of network traffic, but is concerned about compromise of the data stream. Let's say a system under consideration by the integrator has been evaluated that utilizes end-to-end encryption, but not link encryption. As part of the evaluation, it is given a rating of "good" for data confidentiality and a rating of "not present" for traffic flow confidentiality. The "not present" rating does not adversely effect the decision to use that system in this particular environment. Another integrator, however, may feel that traffic flow analysis is a threat and this particular system would not be adequate.

There are constraints on the rating that are applied. First, NCSC requires that in order for the component to be rated above minimum for strength of mechanism, it must protect against deliberate attacks, above and beyond merely accidents and/or malfunctions. Second, the assessment is bounded by the Part I and/or Appendix A evaluation. It is important to note that the other services evaluation cannot be performed without a Part I or Appendix A evaluation. This is because the integrity of the service is dependent on the protection of the NTCB. A standalone evaluation could determine the functionality and, for the most part, the strength of mechanism of the service. However, there is no assurance that the service will not be altered. This assurance is based mostly on the protections provided by the NTCB. NCSC has determined boundary conditions on the ratings which are described in Table 4-2.

Part II Assurance Rating	**Minimum Part I or Appendix A Evaluation**
Minimum	C1
Fair	C2
Good	B2

Table 4-2: Assurance Rating Relationship to TNI Part I

General Assurance Approaches

There is a general approach to determining the assurance of many of the services. When a service is evaluated, the specific assurance rating identified for that service is combined with a general assurance rating to provide the overall rating. The general service factors include the level of software engineering used during design and implementation (e.g., a modular approach, formal methods), the level of testing employed, the level of configuration management, and the existence of a well implemented distribution capability (ensuring that distributed products are up to date and correct).

Documentation

Documentation can be provided either independently for the services or combined with the Part I or Appendix A documentation suite. Documentation must include a: Security Features User's Guide, Trusted Facility Manual, test documentation, and design documentation. This documentation must address those considerations unique to the security service.

Support Primitives

Encryption and protocol primitives are frequently used to implement the other security services. Because of their pervasive use, they are frequently confused as security services in and of themselves. They are, however, simply tools used to yield the security services.

Encryption is used to protect against data compromise, traffic analysis, message stream modification, and masquerading. These threats are commonly brought about by the use of wiretaps. Therefore, encryption is mostly used when the media is unprotected. The strength of mechanism is determined by NSA, based on classified mathematical and statistical analysis, and results in a statement of the highest classification level protected by the mechanism. The adequacy of implementation is also considered when rating the strength of the mechanism. A separate assurance rating is typically not disclosed by NSA.

Protocols provide the communications conventions agreed upon by the peer entities to allow acknowledgments, retransmissions, reconstruction and routing of messages. Therefore, protocols can incorporate provisions to protect against service deficiency, random interference, and malicious interference. Functionality is measured by the amount of service deficiency (e.g., dead locks) inherent in the design of the protocol, the protection against random interference, and protections against malicious interference (e.g., active wiretapping). The strength of mechanism is assessed in relation to design or implementation deficiencies. Assurance is determined by design specification and verification based on a well understood model, and formal testing.

As the services are described in the following paragraphs it will become apparent how the security services rely greatly on various forms of these support primitives.

The Security Services

The three other security services: Communications Integrity Services, Denial of Service Protection, and Compromise Protection are explained in the following paragraphs.

Communications Integrity is supported by the use of authentication, communications field integrity, and non-repudiation techniques.

Authentication ensures that a communications session is established with the intended peer level entity. A common attack is to create a session under a false identity or through playback of a previously legitimate session initiation sequence. Once the false identity is established, the attacker may obtain classified information or may be able to effect unwanted system responses.

This is a recognized threat in the banking industry. An attacker could record a funds transfer into his account. He could then cause that transfer to repeat many times by replaying the session with the sending bank.

The available techniques used for peer authentication are:

- Something known by the entity
- Use of characteristics and/or possessions of the entity
- Cryptographic means

There are several authentication mechanisms available. Passwords (something known by the entity) are commonly used. The use of encryption requires that the communicating entity possess the proper key assigned to itself. Additionally, it defends against playback of previously established legitimate sessions. ATM cards, Smart cards, and datakeys are something that is possessed by the entity. Distinctive characteristics of users can be established through the use of biometric devices (i.e., retinal scanners, handprint scanners, photographs, and voice recognition).

Functionality is rated on the presence of one or more of the techniques mentioned above. Typically, an implemented service will utilize two or more techniques to insure proper authentication (e.g., something you have and something you know). The strength of mechanism is rated according to this implementation. Cryptographic strength of mechanism is supplied by NSA. The general assurance approaches, discussed earlier, are used for an assurance rating.

VSLAN utilizes the DES algorithm to encrypt datagrams and cryptographically bind the addressing and sequencing of datagrams. Subjects are also authenticated by the possession of a data key that is only valid on a particular host. Encryption devices like the XEU and Wang TIU rely on the sending entity having the proper encryption key. Secure Dynamics utilizes an authentication system that requires that the user possess a smart card that generates a pseudo random value in time series lock with a host system.

Communications field integrity (also known as Data Integrity) prevents unauthorized modification of any fields in a communications package. It ensures that the data is accurately transmitted from the source to destination. Data integrity can be compromised by active threats as well as network failure. This service detects the alteration of data and can sometimes recover altered data. It is less concerned with prevention of data alteration. It is generally more important (and safer) to know when data is bad, than to simply rely on prevention techniques. Similar to the banking example used earlier, the attacker could intercept the electronic fund transfer and change the field that specifies the amount of funds to be transferred. The message would then be sent to the receiving bank (with a higher dollar amount). For military applications, there is the danger that missile target data could be changed to disrupt the missiles mission, or a messages security label could be downgraded.

The communications field integrity service is implemented through the use of network protocols and encryption. Network protocols utilize checksums, such as Cyclic Redundancy Checks (CRC's) and framecheck sequences, to detect communications errors and/or changes in data fields. These checksums, however are not strong against malicious threats. The algorithms used are well known and could be reapplied to altered data. The receiving system, then, would believe that the altered data is legitimate. These checksums are useful when protecting against network transmission problems, such as garble. Cryptographically based checksums provide more robust protection against the active wiretapping threat. Because the algorithms are more complex, it is a great deal more difficult to replicate a legitimate packet of data.

The functionality rating of this service based on the granularity of the detection and the possibility of recovery. Strength of mechanism is based on general encryption factors, correctness of protocol logic as well as the adequacy of the particular implementation. The general assurance approaches, discussed earlier, apply to this service.

The VSLAN utilizes DES encryption, packet sequence numbers, as well as underlying Ethernet protocols to provide data integrity. The Wang TIU, BFE and the XEU can provide data integrity using encryption. Attempts to replay packets would be rejected because the encryption key would be incorrect. Also, the encryption of the packets makes it difficult to determine which packets to replay or which fields to alter.

The **Non-repudiation Service** provides unforgeable proof of the shipment and/or receipt of data. This non-repudiation with proof of shipment prevents a sender from falsely denying sending a message. Non-repudiation with proof of delivery prevents a message recipient from denying receipt of a message. In the people/paper world, a signature on a letter or contract that has been notarized commits the author to the letter or contract. Since the author has signed the letter and a notary public has witnessed the signing, denying originating the letter is prevented. Similarly, a certified letter is analogous to the recipient case. The signature acknowledging receipt of the letter provides the sender with proof that the letter was received. An important underlying principle here is that the signature mechanism must be unforgeable and adjudicable. That is one must be able to believe the "signer" actually signed the message and it must be possible for a judge or arbitrator to settle a dispute between the sender and receiver.

The previous analogies both relied on signatures as non-repudiation mechanisms. In the communications world there is a comparable device called the digital signature. The digital signature is unique to the entity that is sending or receiving the data much like a person's signature. Electronic digital signatures typically use public key encryption algorithms. The National Institute of Standards and Technology has presented a draft Federal Information Processing Standard: "Digital Signature Standard" for community review which has created much comment and controversy.

Functionality is rated as present if one or both of the mechanisms are present. Strength of mechanism is based on general encryption factors, correctness of protocol logic as well as the adequacy of the particular implementation. General assurance approaches, as well as encryption and protocol assurance approaches, apply to this service.

The SDNS standard utilizes a Message Security Protocol, residing at OSI layer 7, that provides for proof of origin and receipt.

Denial of Service Protection Services are characterized by Continuity of Operations, Protocol Based Mechanisms, and Network Management. Denial of Service Protection Services concentrate on the assurance of communications availability. This assurance is provided, in increasing levels, by detection, recovery, and/or resistance to Denial of Service conditions. Denial of Service is used to defeat a system by denying communications and preventing it from accomplishing its mission. It can be used as a terrorist attack. As an example, an airport flight tower put out of commission during peak periods could have disastrous results. A network must always deal with the communication anomalies (noise, overloading) that are all too common, and continue to provide the required level of service.

Continuity of Operations is a system's ability to maintain communications during adverse conditions. The system must be robust against single point failures and should be able to continue its mission at an acceptable level during failure conditions. A basic function is the ability to at least report network failure to the system manager so that appropriate measures can be taken to alleviate the problem.

Redundancy of network components can enhance reliability and survivability, reduce single-point of failure, and provide excess capacity. Reconfiguration can work around problem areas by providing alternate communications paths. Network control functions can be distributed statistically and/or dynamically to respond to changing throughput and topology requirements. Fault tolerance mechanisms (such as packet retransmission used in connection-oriented protocols) provide the capability to deal with and recover from network failures. Security controls can be employed to provide isolation and separation of communities of interest so that critical mission functions can continue despite the failure of other areas on the network.

The functionality rating ranges from detection of degradation, to robustness against degradation, to adaptation capabilities. Strength of mechanism is based on rigorous analysis to assure algorithmic correctness in addressing system failures. Assurance is ascertained by simulation, testing, and measurement under extreme conditions.

The Blacker network utilizes an Access Control Center (ACC) and Key Distribution Center (KDC) for network security policy management. If they become unavailable, their functions are distributed amongst BFEs (called "emergency mode") so that the network can continue operating. Many LAN gateways and the Defense Data Network (DDN) IP protocol utilize dynamic routing to provide alternate paths for packets. The Harris Night Hawk can be implemented with two processors and disk shadowing to provide system back-up This would be useful if the Night Hawk was used as a secure router. Because routers are critical to the communications of many systems, the Night Hawk could provide a more robust routing capability due to its ability to reconfigure quickly from disk failure or corruption.

Protocol based mechanisms focus on detection of service denial. This typically involves probing or testing. These mechanisms are commonly implemented using existing protocol features. This is advantageous because this reduces network overhead that could be created by the addition of overlaid Denial of Service mechanisms. It is important that the mechanism not adversely effect network performance thereby exacerbating the condition it was meant to defeat.

Protocol based mechanisms are commonly implemented by health check messages (i.e., "are you alive ?") invoked at regular intervals and/or during idle periods. Time-outs during peer entity "conversations" are also utilized. Additionally, transmission rate may be monitored by a separate process to detect throughput degradation. Alternate routing may be selected when protocols detect performance degradation below a prescribed level or alternately the network administrator may be notified of an impending trouble spot for corrective action.

Functionality is rated based on the number and quality of protocol based mechanisms provided. Network protocol robustness may decrease with network loading, impacting the strength of mechanism. Strength of mechanism is based on rigorous analysis to assure algorithmic correctness in addressing system failures. Assurance is ascertained by simulation, testing, and measurement under extreme conditions.

The VSLAN utilizes a status poll from the Network Security Center to each host on the network. This used by the NSC to provide a health check of each host. In addition, each host utilizes a watchdog timer that detects the loss of the status poll, indicating a NSC failure. Further. the Verdix card in each host provides a status field available to the host so that upper layer protocols may utilize the information. Most commercial TCP/IP based products incorporate timeouts and retransmission functions.

Network Management provides protection beyond that of the previous two protection services. These services concentrated on the detection and handling of throughput degradation at an entity to entity level. Denial of Service can be effected through capacity overload, network flooding, or excessive protocol retry due to excess noise on the channel. Throughput level or network loading could be considered acceptable (albeit close to the limit) between communicating entity pairs, but if this were the case between many entities, the aggregate, network-wide, throughput could effect the overall mission of the system. These are instances that may not be detectable unless a network-wide view is utilized. Further, it may be only possible (or desirable) for a network manager to correct a problem. Network management takes into account these network-wide problems and takes appropriate measures to counteract them.

An example of the use of network management is the case where a peer entity (most critically a network server)is degraded or no-go. The network management function detects the failure and notifies other entities of the failure so that they may make alternate provisions, or it actively repairs the failed entity. This would reduce the amount of retransmissions and protocol unique packets on the network as well as speed up the recovery process. It should be noted that network peer entities may have detected the failure but were unable to effect the repair or change in network configuration.

The functionality of this service is rated as none or present based on the mechanisms mentioned above. Network management mechanism strength may decrease inversely with network loading. Assurance is based on the general assurance factors discussed earlier.

The Verdix NSC detects status changes of nodes, tracks packet integrity errors and generates alarms after limits are exceeded, and can shutdown or suspend nodes that are suspected of creating problems on the network.

Compromise Protection Services include data confidentiality, traffic flow confidentiality, and selective routing.

Data confidentiality addresses the unauthorized direct disclosure of data. That is, the observation of the actual data through passive wiretap. Passive wiretap can be effected through the use of LAN analyzers, or connection of a simple computer with compatible network software and hardware.

The most common use of encryption technology is to provide a data confidentiality service. End-to-end encryption (at layer 4) provides confidentiality between two entities while allowing normal network routing due to layer 3 and lower headers being unencrypted. This also allows cohabitation on a broadcast network with non-encrypted systems since the layer 3 and below headers are readable and the encrypted packet can be treated like any other network packet by other entities, network routers, and bridges.

Functionality is rated on the presence or absence of data confidentiality for all user data on a specific protocol layer connection, all user data in a single connectionless datagram, or selected fields within the user data of a PDU. Strength of mechanism measurement is beyond the scope of the TNI. Assurance approaches are consistent with the general approach described earlier.

The Wang TIU, Xerox XEU, Motorola NES , SDNS standard (in the SP3 protocol) and Blacker provide end-to-end encryption. Blacker has addressed assurance by hosting on an evaluated (A1) TCB.

Traffic confidentiality addresses the unauthorized indirect disclosure of data through inference by observation and analysis of message length, frequency, and source/destination addresses. This is accomplished through the use of passive wiretapping. One use of this information could be to determine the critical, highly used links and then dedicate resources to defeating those links. Large packets, indicating data transfer, to a particular site could indicate the deployment of assets from that site. Traffic from a front-line listening post could be monitored. Traffic from the listening post would indicate it is reporting an event. The event level would be raised until packets from the listening post were detected, thereby calibrating the listening posts detection capability.

Encryption of the OSI data link layer (i.e., link encryption) is used for this service to mask the source destination pair used for network routing. Traffic padding is the transmission of "dummy" packets on the network to disguise any characteristic frequency by creating a constant level of network traffic. Message length padding masks the characteristics of individual packets. It should be noted that Denial of Service considerations must be taken into account due to the additional loading on the network caused by message length and traffic padding.

The functionality assessment is based on the presence or absence of the mechanisms mentioned above. The strength of mechanism rating is considered out of scope of the TNI. Assurance approaches are consistent with the general approach described earlier.

KG-84s provide link encryption and are required, typically, in a Blacker network. SDNS has provisions for link encryption in the SP2 protocol.

Selective routing is used to select or avoid specific transmission routes. This can be used to avoid routes that are higher risk. It also is utilized to restrict labeled data from transmission through certain links according to the system security policy.

Routes can be chosen either dynamically or statically through prearrangement. Dynamic routing would be used when a specific link is known or suspected to be compromised. Prearranged routing restrictions may be due to links that are known to be protected in varying degrees. World-wide communications could avoid certain hostile countries. National laws and network administration policies govern individual privacy rights, encryption, and trans-border data flow.

Functionality is based on the presence or absence of the mechanisms mentioned above. The strength of mechanism rating is consistent with the factors discussed under support primitives. Assurance approaches are consistent with the general approach described earlier.

The Defense Data Network imposes selective routing. The Harris Night Hawk has the capability to provide secure routing between connected separate LANs. Hosts on different LANs are allowed to communicate based on host Access

Control Lists as well as security level. Security level is determined either by the level of the LAN on which the host resides or by packet labels (CIPSO, RIPSO, or VSLAN).

<u>Required Readings</u>

The required readings are supplied as part of the source material for the module. These readings, and the module overview, provide all the material covered by the module test questions.

DTNI87 National Computer Security Center, *Trusted Network Interpretation of The Trusted Computer System Evaluation Criteria*, NCSC-TG-005, 31 July 1987.

The TNI provides an interpretation of the requirements stated in the TCSEC for the evaluation of trusted network systems. Part II describes other security services and should be read for this module.

<u>Other Related Readings</u>

DEPL90 National Computer Security Center, *Final Evaluation Report, Verdix Corporation, VSLAN 5.0*, CSC-EPL-90/001, 25 July 1990.

DEPL91 National Computer Security Center, *Final Evaluation Report, Boeing Space and Defense Group, MLSLAN Secure Network Server System*, CSC-EPL-91/005, 28 August 1991.

JSTO89 12th National Computer Security Conference Proceedings, *"The Boeing MLS LAN: Headed Towards an Infosec Security Solution"*, G. Stoneburner, 1989.